

**ORIGINAL, FÄLSCHUNG ODER VON
DER KI ERSTELLT?**

AUTHENTIFIZIERUNG DIGITALER INHALTE MIT WEB3-TECHNOLOGIEN

Der vorliegende Deepdive des Web3-Thinktank zeigt auf, wie Web3-Technologien zur Authentifizierung digitaler Inhalte das Vertrauen in Content stärken können – insbesondere angesichts der Gefahr von Desinformation durch Künstliche Intelligenz.

Der Deepdive gibt eine Erklärung, wie Content-Authentifizierung funktioniert, indem digitale Inhalte mit einem kryptografischen Fingerabdruck und Metadaten über ihre Herkunft und Bearbeitung versehen werden. Diese Daten werden dann

auf öffentlichen Blockchains gesichert. Außerdem werden Initiativen und Projekte vorgestellt, die an zukunftsweisenden Modellen zur Content-Authentifizierung arbeiten, darunter die Content Authenticity Initiative (CAI), das amerikanische Starling Lab oder das Berliner Startup Valid. Anhand von Beispielen aus der journalistischen Praxis zeigt der Deepdive, wie Web3-Technologien bereits zur Content-Authentifizierung angewendet werden, etwa bei der Dokumentation des Kriegs in der Ukraine oder des Sturms auf das Kapitol in den USA.

INHALTS- VERZEICHNIS

VORWORT	3
WAHRHEIT IM INTERNET UND DIE ROLLE VON WEB3-TECHNOLOGIEN	
DIE HERAUSFORDERUNG	4
NOCH MEHR DESINFORMATION MITHILFE VON KÜNSTLICHER INTELLIGENZ?	
MÖGLICHE LÖSUNGEN?	5
FRAGEN UND ANTWORTEN ZU WEB3-TECHNOLOGIEN ZUR AUTHENTIFIZIERUNG VON DIGITALEN INHALTEN	
CONTENT AUTHENTIFIZIERUNG MIT WEB3-TECHNOLOGIEN IN DER PRAXIS	8
FALLBEISPIEL 1	
• Fotos mit Echtheitszertifikat: Die Arbeit des Starling Labs	
FALLBEISPIEL 2	
• Authentifizierung von Nachrichtenartikeln mit Valid	
FALLBEISPIEL 3	
• In der Wissenschaft im Alltagseinsatz: Die Bloxberg-Blockchain aus München	
FAZIT UND AUSBLICK	13
TECHNOLOGIE ALLEIN WIRD DIE HERAUSFORDERUNG NICHT LÖSEN	
ÜBER UNS	14
VERZEICHNIS	15

VORWORT

Jacqueline Hoffmann, Leitung des Web3-Thinktanks

WAHRHEIT IM INTERNET UND DIE ROLLE VON WEB3-TECHNOLOGIEN

Bei den MEDIENTAGEN MÜNCHEN 2022 war das Thema Web3 mit einem eigenen Programm-Track und der Veröffentlichung der Studie „Web3: Was kommt auf die Medienbranche zu?“ prominent platziert – und die Rückmeldungen aus der Branche waren eindeutig: Viele Unternehmen wollten sich intensiver damit beschäftigen, was Blockchains, NFTs, Dezentrale Autonome Organisationen, Communities oder dezentrale Apps – die zentralen Bausteine des Web3 – für sie bedeuten könnten, was mögliche Use Cases sind und was nicht. Mit dem neugegründeten Web3-Thinktank schuf das MedienNetzwerk Bayern ein Angebot, um die Branche bei der Beantwortung genau dieser Fragen zu unterstützen.

Im Rahmen von Workshops, Meetups und digitalen Sessions kristallisierte sich heraus, dass viele Medienunternehmen – vom TV-Anbieter bis zur Regionalzeitung – großen Bedarf sehen, etwas gegen die Flut an Desinformationen und Fake News in den sozialen Medien zu tun. Insbesondere, da es durch generative Künstliche Intelligenz, also durch ChatGPT, Midjourney und andere Programme, noch einfacher geworden ist, täuschend echte, aber falsche und nicht authentische Inhalte zu erzeugen.

Die Medienhäuser, mit denen sich der Web3-Thinktank zu diesem Thema austauschte, sahen dabei auch das Potenzial von Web3-Technologien, zu einer Lösung beizutragen. Denn die Verbindung aus Kryptografie und Blockchains macht es möglich, digitale Inhalte mit einer Art Echtheitszertifikat

zu versehen. Nutzer:innen können so schnell und einfach herausfinden, wer, wann und wo einen bestimmten Inhalt erstellt und veröffentlicht hat. Zahlreiche Tools und Technologien sind bereits in der Entwicklung und teilweise im Praxiseinsatz.

Der vorliegende Deepdive gibt Medienschaffenden und -unternehmen einen tieferen Einblick in die Möglichkeiten, digitalen Content mit Web3-Technologien zu authentifizieren. Dabei wird dargelegt, warum generative Künstliche Intelligenz den Bedarf nach derartigen Lösungen noch vergrößert hat. Außerdem werden grundsätzliche Fragen dazu geklärt, wie das Web3 zu mehr Transparenz und Vertrauen in digitale Inhalte führen kann. Anschließend werden drei Beispiele vorgestellt, die konkrete Tools und Technologien bereits einsetzen und Medienhäusern die Möglichkeit geben, diese zu erproben. Das Whitepaper endet mit einem Ausblick und einer Einordnung der Rolle von Web3-Technologien im Hinblick auf einen gesunden öffentlichen Diskurs.

Sollten Sie nach Lektüre des Deepdives weitere Fragen oder Interesse haben, in Pilotprojekten Content-Authentifizierungs-Lösungen zu implementieren, nehmen Sie gerne Kontakt zum Web3-Thinktank des MedienNetzwerks Bayern auf. Auch zu anderen Fragen rund um Einsatzmöglichkeiten von Web3-Technologien in der Medienbranche liefert der Thinktank nicht nur Informationen, sondern bietet auch Workshop-Formate an, um mögliche Use Cases für das eigene Haus zu identifizieren.

DIE HERAUSFORDERUNG

NOCH MEHR DESINFORMATION MITHILFE VON KÜNSTLICHER INTELLIGENZ?

Wird das Internet bald von Fake-Inhalten überflutet, die von Künstlichen Intelligenzen erzeugt wurden? Das Risiko besteht, denn ChatGPT, Stable Diffusion & Co. lassen sich auch zur Desinformation missbrauchen.

Nicht jede falsche Information, die in einem Artikel, Podcast oder Video verbreitet wird, ist eine Form von Desinformation. Denn in Redaktionen passieren Fehler, die dann korrigiert werden. In diesem Fall wird von Fehlinformation gesprochen. Desinformation meint falsche Informationen, die gezielt gestreut werden, zum Beispiel um Einfluss auf politische Wahlen zu nehmen oder aus betrügerischer Absicht. Sie kann in vielen Formen auftreten. Manipulierte Fotos und Videos, glaubhaft klingende, aber manipulative Texte oder Zitate und Aufnahmen, die völlig aus dem Kontext gerissen werden – all das kursiert seit Jahren in den sozialen Netzwerken, schon bevor generative Künstliche Intelligenz ihren Durchbruch erlebte.

Im Jahr 2022 tauchten sogar Dutzende gefälschter Nachrichtenseiten auf, die zum Beispiel prorussische Propaganda oder Werbung für unseriöse Bitcoin-Geschäfte verbreiteten. Die Seiten sahen aus wie die Angebote etablierter Medien – Tageschau, Welt, Bild, t-online – und hatten teils ähnliche klingende Domains. Selbst für derart aufwendige Kampagnen braucht es keine sogenannte generative KI, womit Künstliche Intelligenz gemeint ist, die digitale Inhalte erstellen kann. Doch Programme wie ChatGPT oder Stable Diffusion, aber auch Deepfake-Technologien machen es einfacher, synthetische Inhalte zu produzieren, die echt wirken. KI könnte also zu mehr und gezielterer Desinformation führen.

Den Anfang machten KI-Deepfakes, also Videos oder Sprachaufnahmen, in denen täuschend echt aussehende oder klingende Personen etwas sagen oder tun – ohne, dass dies je stattgefunden hat. Obwohl die Produktion von Deepfakes für Laien ohne ausführliche YouTube-Tutorials oder Tipps aus Onlineforen kaum möglich war, kursierten bereits 2017 pornografische Videos im Netz, in denen die Gesichter der Darstellerinnen mit denen bekannter Schauspielerinnen ersetzt worden waren.

Zum Massenphänomen wurde die Erstellung synthetischer Inhalte per KI dann ab 2021 mit Bildgeneratoren wie DALL-E, Stable Diffusion oder Midjourney und Textgeneratoren wie ChatGPT, BARD oder Bing. Um mit diesen Tools realistische Bilder oder plausibel klingende Texte zu erzeugen, braucht es keine Programmierkenntnisse. Die Programme werden per Texteingabe, mit Prompts, bedient. Das gilt auch für Audio- und Videogeneratoren, die gerade große Fortschritte machen.

Die Warnungen, dass KI zur Desinformation eingesetzt werden kann, wurden mit jedem technischen Entwicklungsschritt lauter. Schon 2020 prognostizierte die Autorin Nina Schick in ihrem weltweit beachteten Buch „Deepfakes: The Coming Infocalypse“, dass bis 2030 über 90 Prozent aller Inhalte im Internet synthetisch sein werden. Inzwischen wird auch auf den Seiten der Bundesregierung, von Europol und selbst von OpenAI, der Firma hinter ChatGPT, vor dem Missbrauch von generativer KI gewarnt. Die Universität Zürich fand heraus, dass Twitter-Nutzer:innen KI-generierte Desinformationen eher für wahr hielten als menschengemachte. Erschwerend kommt hinzu, dass KI-Chatbots zum „Halluzinieren“ neigen, das heißt, sie geben schlüssig erscheinende, jedoch faktisch falsche Antworten auf Fragen.

Durch KI könnte also ein Problem noch drängender werden, das viele Menschen ohnehin schon besorgt: Im Frühjahr 2023 gaben bei einer EU-weiten Umfrage im Auftrag der Bertelsmann Stiftung 54 Prozent der Befragten an, in den letzten Monaten häufig oder sehr häufig verunsichert gewesen zu sein, ob Informationen im Internet wahr sind oder nicht. 39 Prozent sagten, häufig oder sehr häufig Desinformationen im Internet wahrgenommen zu haben. Und über 80 Prozent waren der Meinung, Politik und Internetplattformen müssten stärker dagegen vorgehen.

MÖGLICHE LÖSUNGEN?

FRAGEN UND ANTWORTEN ZU WEB3-TECHNOLOGIEN ZUR AUTHENTIFIZIERUNG VON DIGITALEN INHALTEN

Weltweit überprüfen professionelle Fact-Checking-Teams die Authentizität digitaler Inhalte – von Fotos, Videos, Texten. Schon für diese Profis ist es oft schwierig, die Vertrauenswürdigkeit von Content einzuschätzen. Für User:innen ohne Fachwissen ist es manchmal fast unmöglich. Wer ist der Urheber der Inhalte? Wurden sie tatsächlich zu diesem Zeitpunkt an diesem Ort aufgenommen? Und wurden sie nachbearbeitet? Web3-Lösungen auf Basis von Kryptografie und Blockchains sollen künftig für mehr Transparenz sorgen. Wir beantworten die wichtigsten Fragen dazu.

Warum braucht es neue Lösungen zur Authentifizierung von digitalem Content?

In der Kunstwelt ist es längst selbstverständlich, sich vor dem Kauf eines Werkes über seine Provenienz, also seine Herkunftsgeschichte zu informieren. Wem gehörte die Arbeit zuvor? Kann die Echtheit garantiert werden? Oder handelt es sich gar um ein illegal erworbenes Stück? Das zu klären, kostet Zeit – die beim Handel mit Kunstwerken meist vorhanden ist. Auch der digitalen Öffentlichkeit könnte Klarheit über die Vertrauenswürdigkeit



Bild: The Pope Drip - KI-generiertes Bild des Papstes - Screenshot von Reddit

digitaler Inhalte helfen, sagt nicht zuletzt die EU-Kommission. Doch anders als in der Kunstwelt nimmt sich für ausgiebige Provenienzforschung kaum jemand Zeit. Ein harmloses Beispiel aus dem Frühjahr 2023 verdeutlichte das einmal mehr: Über alle sozialen Netzwerke verbreitete sich ein „Foto“, das Papst Franziskus in einer stylischen Daunenjacke zeigte.

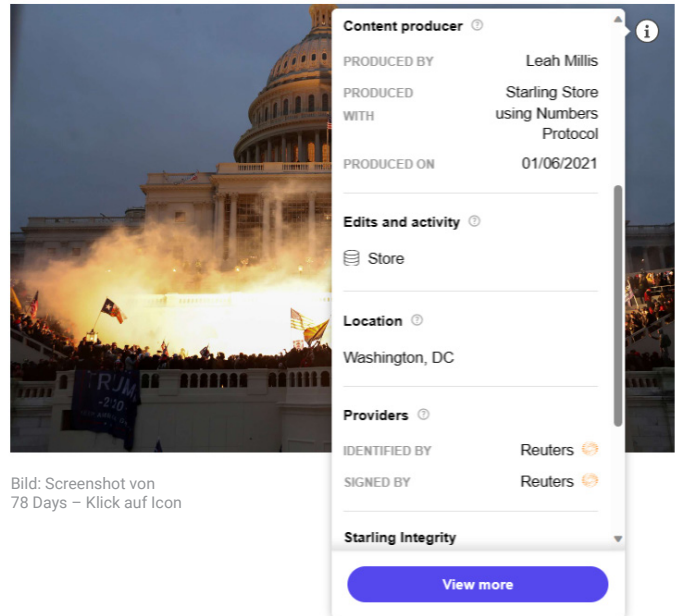
Manchen User:innen fiel schnell auf, dass mit dem Bild etwas nicht stimmte – die jugendlichen Hände passten nicht zum Alter des Papstes. Viele andere feierten ihn hingegen als hippen Mode-Influencer. Denn die Information, dass das Bild mit dem KI-Bild-generator Midjourney erschaffen wurde, ging erst mit Verzögerung „viral“ – obwohl die Darstellung ursprünglich sogar mit dem klaren Hinweis darauf bei Reddit veröffentlicht worden war.

Der Fall war für viele ein Weckruf, dass es neue Lösungen braucht, um schnell und unkompliziert überprüfen zu können, ob Content authentisch ist. Sonst könnte das Vertrauen in digitale Inhalte weiter schwinden. Zumal das KI-generierte Bild des Papstes harmlos war. Fotos, Videos, Audios oder Texte, die angeblich politische Ereignisse, Kriegshandlungen oder Verbrechen dokumentieren, aber mit KI erstellt oder auf klassischem Wege gefälscht bzw. ihres wahren Kontextes beraubt wurden, könnten für die Demokratie zur Gefahr werden.

Um Nutzer:innen mit Informationen über die Herkunft und Authentizität von Inhalten versorgen zu können, arbeiten Organisationen, Forschungseinrichtungen und Unternehmen an verschiedenen, in ihrem Grundsatz jedoch häufig ähnlichen Lösungen. Meist verfolgen die entstehenden Tools einen Open-Source-Ansatz, zum Teil basieren sie auf Web3-Technologien wie dezentralen Netzwerken – also: Blockchains – und Kryptografie.

Wie könnten neue Tools, die für mehr Vertrauen sorgen, aus User-Sicht funktionieren?

Ziel dieser Tools ist es, so unkompliziert wie möglich Informationen über die Provenienz des Contents zu liefern – direkt im Social-Media-Feed oder auf den Webseiten von Inhalte-Anbietern. Über einen Klick auf ein Icon in der Ecke von Bildern und Videos bzw. neben der Überschrift von Artikeln sollen die Informationen abrufbar sein. Icons können zum Beispiel ein kleines „i“ oder die Buchstaben „cr“ (steht für Content Credentials) in einem Kreis sein, oder ein grüner Haken. Mit Klick auf das Icon können User:innen innerhalb von Sekunden feststellen, ob ein Inhalt KI-generiert ist oder nicht, von wem er stammt oder wann und wo er erstellt oder bearbeitet wurde. Eine Aussage, ob der Inhalt wahr oder falsch ist, liefern die Tools allerdings nicht – schließlich durchlaufen die Inhalte keinen Faktencheck. Dennoch bieten sie wertvolle Anhaltspunkte, um die Vertrauenswürdigkeit und Authentizität des Inhalts beurteilen zu können.



Wie funktionieren Web3-Lösungen technisch?

Im Prinzip funktionieren die meisten Lösungen in drei vergleichbaren Schritten:

1

ERSTELLEN:

Inhalte erhalten sofort nach ihrer Erstellung einen digitalen Fingerabdruck. Dafür werden sie von ihren Urheber:innen signiert und je nach Bedarf mit Informationen darüber versehen, von wem, wo, wann und mit welcher Hard- oder Software sie erstellt wurden. Außerdem wird den Inhalten per kryptografischem Verfahren ein sogenannter Hashwert zugeordnet, weshalb der Arbeitsschritt auch „Hashing and Signing“ genannt wird. Bearbeitungen der digitalen Inhalte werden auf dieselbe Art festgehalten, ebenso die Informationen, wer den Inhalt veröffentlicht. Basierend auf dem Standard der Coalition for Content Provenance and Authenticity, kurz C2PA, kann der digitale Fingerabdruck inklusive aller Metadaten – auch als „Content Credentials“ bezeichnet – bei Bildern, Videos und Audios direkt in die jeweilige Datei eingebettet werden. Die Datei wird zum Container für Provenienz-Informationen.

2

SPEICHERN:

Für zusätzliche Sicherheit wird der digitale Fingerabdruck der digitalen Inhalte, der aus Hashwert, Signatur und Metadaten besteht, auf einer öffentlichen Blockchain gespeichert. Dabei handelt es sich um ein dezentrales Netzwerk, dessen Inhalte, anders als bei einem zentralen Server, nur sehr schwer manipulierbar sind. Zusätzlich besteht die Möglichkeit, die digitalen Inhalte selbst auf dezentralen Peer-to-Peer-Netzwerken wie IPFS, Filecoin oder Storj zu sichern, die teils ebenfalls auf Blockchain-Technologie beruhen. Das schützt beispielsweise Inhalte von historischer Bedeutung zusätzlich vor Löschung oder Manipulation. Auch der Verweis auf die Blockchain-Einträge und Speicherorte lässt sich unter Verwendung des C2PA-Standards in die Bild-, Audio- oder Videodatei selbst integrieren.

3

VERIFIZIEREN:

Stoßen Nutzer:innen in sozialen Netzwerken oder auf Webseiten auf digitale Inhalte, können sie die Informationen zur Provenienz und damit zur Authentizität abrufen – zum Beispiel per Klick auf ein Icon, wie oben beschrieben. Voraussetzung dafür ist, dass der Betreiber der jeweiligen Plattform dies ermöglicht. Zusätzliche Transparenz schafft die Möglichkeit, die unterschiedlichen Versionen eines digitalen Inhalts zu vergleichen. Für Bilder, die basierend auf dem C2PA-Standard mit Provenienz-Informationen versehen wurden, lässt sich dafür bereits das Tool Verify nutzen.

Gibt es bei diesen Lösungen auch dann eine Möglichkeit, digitale Inhalte zu überprüfen, wenn sie keine Metadaten mehr enthalten?

Ja, über den Hashwert. Für den im Netz gefundenen Inhalt ohne sofort verfügbare Provenienz-Informationen kann ein Hashwert ermittelt werden. Ist dieser mit dem Hashwert des Originals, der zum Beispiel auf einer Blockchain gesichert wurde, identisch, ist auch der Inhalt authentisch und wurde nicht nachträglich manipuliert. Wurde der Inhalt jedoch verändert, stimmen die beiden Hashwerte nicht überein. Dafür reicht schon die Manipulation eines einzelnen Pixels.

Was hat es mit dem Standard der Coalition for Content Provenance and Authenticity (C2PA) auf sich?

Die Coalition for Content Provenance and Authenticity, kurz C2PA, bündelt die Arbeit zweier, von Unternehmen vorangetriebenen Initiativen: der Content Authenticity Initiative (CAI), die 2019 unter anderem von Adobe, der New York Times und Twitter gegründet wurde, sowie des Project Origin, 2018 gestartet von Microsoft, der BBC und anderen. Beide Initiativen haben es sich zum Ziel gesetzt, Desinformation und Vertrauensverlust zu bekämpfen, indem digitale Inhalte mit Informationen zu Provenienz und Authentizität versehen werden.

Die C2PA hat die Aufgabe, einen Open-Source-Industriestandard zu entwickeln, auf dessen Basis konkrete Tools und Lösungen gebaut werden können. Die von der C2PA bereitgestellten technischen Spezifikationen dafür, wie Metadaten und Signaturen unter Anwendung kryptografischer Methoden an digitale Inhalte gekoppelt werden, wurden bereits unter Creative Commons Lizenz CC BY 4.0 veröffentlicht. Sie können daher verwendet werden, ohne Lizenzzahlungen leisten zu müssen.

Wer treibt die Entwicklung von Lösungen zur Content-Authentifizierung voran?

Der wichtigste Player dürfte die bereits genannte CAI sein, die maßgeblich vom Technologieunternehmen Adobe vorangetrieben wurde und wird. Auch deutsche Medien wie Axel Springer, dpa oder Stern gehören der CAI an. Zusammen mit dem Project Origin formte die CAI die zuvor vorgestellte C2PA.

Zentrale Beiträge zur praktischen Implementierung und Kombinationen der verschiedenen Content-Authentifizierungstechnologien und insbesondere auch von Web3-Lösungen leistet das US-amerikanische Starling Lab, das von der Stanford University und der USC Shoah Foundation gegründet wurde. In Projekten mit Reuters, dem Rolling Stone und anderen Partnern entwickelte das Lab Tools für den Praxiseinsatz in Redaktionen.

Verschiedene Web3-Projekte und -Unternehmen bieten ebenfalls Lösungen an, die sich speziell an Medien richten und der Content-Authentifizierung dienen sollen. Dazu gehört das Berliner Startup Valid, das sich auf die Authentifizierung von Artikeln spezialisiert hat. Nodle, ein Anbieter von dezentraler Infrastruktur und Mitglied der CAI, arbeitet mit ContentSign an einer konkreten Lösung für Bilder und Videos. In den Niederlanden entsteht mit Liccium ein Blockchain-Tool, um die Echtheit sowie die Urheberrechte an digitalen Inhalten zu verifizieren.

Können Publisher die Lösungen zur Content-Authentifizierung bereits implementieren?

Im Prinzip ja. Erste Hard- und Software, die mit dem C2PA-Standard arbeiten bzw. „CAI-konform“ sind – benannt nach der Content Authenticity Initiative –, sind bereits auf dem Markt. So existiert mit Truepics Lens eine Software, die es ermöglicht, mit Smartphones aufgenommene Fotos zu signieren und mit ihrem digitalen Fingerabdruck zu versehen. Die Kamerahersteller Canon, Nikon und Leica sind der Content Authenticity Initiative beigetreten und haben Kameras angekündigt bzw. bereits als Prototypen präsentiert, die das ebenfalls können. Software von Adobe, insbesondere Photoshop, ist ebenfalls CAI-konform, wodurch auch Nachbearbeitungen von digitalen Inhalten, zum Beispiel Farbkorrekturen und Zuschnitte, oder die Erstellung von KI-Inhalten dokumentiert werden können.

Wenn die implementierten Lösungen durch den Einsatz der Blockchain-Technologie dezentral und noch sicherer sein sollen, existieren auch dafür bereits Frameworks und Workflows, auf die Publisher aufbauen können. Diese wurden zum Beispiel vom amerikanischen Starling Lab zusammen mit Partnern aus der Medienbranche oder dem Berliner Startup Valid entwickelt, das noch näher vorgestellt wird.

Braucht es für die Content-Authentifizierung unbedingt Web3-Technologien?

Zählt man kryptografische Verfahren zu den Web3-Technologien: ja. Zählt man diese nicht dazu, sondern bezieht sich vor allem auf die Blockchain-Technologie und andere dezentrale Lösungen: nein. Doch bieten sie nach Ansicht von Expert:innen, zum Beispiel von Starling Lab oder Valid, zusätzliche Sicherheit und Transparenz.

CONTENT AUTHENTIFIZIERUNG MIT WEB3-TECHNOLOGIEN IN DER PRAXIS

FALLBEISPIEL 1

FOTOS MIT ECHTHEITSZERTIFIKAT: DIE ARBEIT DES STARLING LABS

Bei der Entwicklung sowie beim Einsatz von Open-Source-Tools und Web3-Technologien zur Authentifizierung von digitalem Content zählt das US-amerikanische Starling Lab, gegründet von der Stanford University sowie der USC Shoah Foundation, zu den führenden Organisationen. In Pilotprojekten mit großen Medienhäusern und Publikationen wie Reuters, dem Rolling Stone oder der South China Morning Post konnten bereits konkrete Workflows implementiert werden. Der Web3-Thinktank hat mit Adam Rose, dem COO des Labs, gesprochen und beleuchtet dessen Arbeit.

Bei den bisher umgesetzten Projekten des Starling Labs standen historische oder aktuelle Ereignisse im Mittelpunkt, die mit digitalen Inhalten – insbesondere Fotos – für die aktuelle Berichterstattung, aber auch für die zukünftige Geschichtsschreibung festgehalten werden sollten. Die Themen hatten darüber hinaus eine weitere Gemeinsamkeit, wie Adam Rose, der Chief Operating Officer des Starling Labs, erklärt: „Wir haben Themen gewählt, bei denen es wahrscheinlich war, dass Tatsachen infrage gestellt, Desinformationen gezielt gestreut oder Belege verschwinden könnten.“

Unter dem Titel „78 Days“ schufen das Starling Lab und Reuters ein digitales Fotoarchiv, das den Zeitraum zwischen der amerikanischen Präsidentschaftswahl im November 2020, die Donald Trump verlor, und der Amtseinführung Joe Bidens im Januar 2021 dokumentierte – inklusive des Sturms auf das Kapitol am 6. Januar 2021. Im Projekt „The DJ and the War Crimes“, das in Zusammenarbeit mit dem Rolling Stone realisiert wurde, beschäftigte sich das Lab mit bis heute ungeklärten Kriegsverbrechen während des Bosnienkriegs im Jahr 1992. Gerade wurden außerdem die Ergebnisse einer weiteren Kooperation mit Reuters und Canon vorgestellt, in deren Rahmen eine Fotografin die Folgen des russischen Kriegs gegen die Ukraine festhielt.

Bild: Screenshot Rolling Stone DJ and War Crime



Dem Starling Lab geht es bei seiner Arbeit um das Schaffen von Datenintegrität. Das bedeutet einerseits, digitale Daten wie Fotos, Videos, Artikel, Webseiten, VR-Experiences zu sichern, zum Beispiel für journalistische Berichterstattung, für Ermittlungsverfahren, für die Geschichtsschreibung. Andererseits geht es darum, diese Daten mit einer Art Authentizitäts-Zertifikat zu versehen, also mit Informationen zur Provenienz: Wo sind sie entstanden? Wer ist der Urheber? Wie wurden sie nachträglich bearbeitet? „Unsere Mission ist es, sicherzustellen, dass Fachleute und das breite Publikum Daten vertrauen können“, sagt Adam Rose.

Um konkrete Tools und Lösungen zu bauen, die diese Datenintegrität in der Praxis gewährleisten, setzt das Starling

Lab auf angewandte Forschung und die Kooperation mit anderen Organisationen, zum Beispiel mit Medienhäusern. Zentral für die bisher entwickelten Lösungen waren neben den Spezifikationen der C2PA auch Web3-Technologien wie Kryptografie, Blockchains oder dezentrale Datenbanken.

Das neueste Projekt: Fotos aus dem Krieg in der Ukraine

Anhand des jüngsten Projekts des Starling Labs mit Reuters und Canon lässt sich beschreiben, wie fortgeschritten die Möglichkeiten der Content-Authentifizierung inzwischen sind. Ziel des Projekts war es, die gesamte Provenienz von Fotos – vom Moment der Aufnahme bis zur Veröffentlichung – transparent zu dokumentieren und für die Öffentlichkeit nachvollziehbar zu machen.

Ganz konkret reiste die Reuters-Fotojournalistin Violeta Santos Moura durch die Ukraine, um mit einem Kamera-Prototyp Fotos der Kriegszerstörungen aufzunehmen. Die Fotos wurden dabei von der Kamera direkt nach der Aufnahme mit Uhrzeit, Standortdaten sowie einem einzigartigen Hashwert versehen und kryptografisch signiert. „Wir sind der Ansicht, dass das Hashing und Signing so nah wie möglich am Ursprung der Daten passieren muss“, erklärt dazu Adam Rose. „Lässt sich eine Signatur mit Software auf dem Smartphone erzeugen, ist das schon ganz gut. Noch besser ist, wenn dies über die Firmware des Gerätes erfolgt. Und am besten ist es, wenn diese Funktionen direkt in die Hardware implementiert sind.“

Die signierten Bilder wurden daraufhin unmittelbar von der Kamera an das Daten-Management-System von Reuters gesendet und der digitaler Fingerabdruck auf einer oder mehreren öffentlichen Blockchains registriert. Für die Registrierung setzt das Projekt auf Open-Timestamps auf der Bitcoin-Blockchain, das Numbers-Protokoll auf der Numbers- sowie der Avalanche-Blockchain und auf ISCN auf der LikecoinBlockchain. Zusätzlich wurden die Bilder auf den dezentralen Archiven IPFS, Filecoin und Storj gespeichert.

Die Redakteur:innen bei Reuters bearbeiteten im nächsten Schritt die Bilder, wobei jede Änderung, zum Beispiel eine Farbkorrektur, einen Eintrag in einer privaten Blockchain-Datenbank von ProvenDB erzeugte. Gleichzeitig wurde auf die ursprüngliche Registrierung auf der öffentlichen Blockchain verwiesen. So konnten die konkreten Änderungsprotokolle privat gehalten werden, während die Authentizitätsnachweise auf der öffentlichen Hedera-Blockchain festgehalten wurden.

Die Veröffentlichung der fertigen Bilder erfolgte schließlich mit allen Informationen über Entstehungszeit, Ort, Blockchain-Registrierungen und Nachbearbeitungen. Diese Metadaten werden über den C2PA-Standard direkt in die JPEG-Datei eingebettet und sind dementsprechend schnell verfügbar. Darüber hinaus können Nutzer:innen die ursprüngliche Version der Bilder über das Verify-Tool der Content Authenticity Initiative mit der nachbearbeiteten, veröffentlichten Version vergleichen.

Web3-Technologien sorgen für zusätzliche Sicherheit und Transparenz

Das Framework und die Tools, die das Starling Lab entwickelt hat, umfassen die drei Arbeitsschritte Capture, Store und Verify: Erstellen bzw. Aufnehmen, Speichern und Verifizieren. Zum Teil können diese Schritte überlappen, zum Beispiel, wenn digitale Inhalte nachbearbeitet werden. Um Datenintegrität zu schaffen, müssen alle drei Schritte transparent nachvollziehbar sein und Manipulationen ausgeschlossen werden.

„Wir sind in der Lage, die Hashes und Daten nicht nur in einer, sondern in mehreren Blockchains zu registrieren, wodurch diese Informationen nicht manipuliert werden können. Außerdem können wir multiple Backups der verschiedenen Versionen von Bildern erstellen, die unveränderlich sind, weil manipulierte Kopien nicht mit allen Versionen übereinstimmen“, erklärt Adam Rose. „Dabei kombinieren wir Open-Source-Tools, die Spezifikationen der C2PA und Web3-Technologien, die hier wirklich entscheidend sind. Erst durch den Einsatz von Kryptografie, dezentralen Speichermethoden und Blockchains können wir sicherstellen, dass Daten langfristig gesichert sind und nicht manipuliert werden können.“

Entscheidet sich ein Medienunternehmen dafür, das Content-Authenticity-Framework des Starling Labs in seine eigenen Workflows zu implementieren, sei das sicher nicht innerhalb von 24 Stunden möglich. Es brauche Anpassungen an die eigenen Bedürfnisse und die Einbindung in Systeme, was durchaus einige Wochen dauern kann. „Aber wenn das System einmal steht und Teil der Arbeitsroutine wird, fühlt es sich ganz natürlich an“, meint Adam Rose.

Wichtig ist dem Starling Lab, dass die Lösungen, die es entwickelt, immer Opt-In-Charakter haben, also nicht obligatorisch sein sollten. Auch Regierungen sollten nicht vorschreiben, auf Fotos vermerken zu müssen, wo, wann und von wem sie gemacht und veröffentlicht wurden: „Werden zum Beispiel Demonstrationen für Frauenrechte im Iran festgehalten, könnten solche Informationen in den Händen der Regierung die Sicherheit von Menschen gefährden.“



Bild: Screenshot von Verify zum Reuters-Prototypen

FALLBEISPIEL 2

AUTHENTIFIZIERUNG VON NACHRICHTENARTIKELN MIT VALID

Das Berliner Startup Valid will Web3-Technologien nutzen, um die Authentifizierung von Nachrichtenartikeln zu ermöglichen. Das Projekt wurde am European Blockchain Center in Kopenhagen ins Leben gerufen. Das Unternehmen plant ein Pilotprojekt mit einem regionalen Verlag aus Deutschland. Im Interview mit dem Web3-Thinktank verraten die Mitgründer und Brüder Hans und Jens Brorsen mehr über ihre Lösung.

Warum ist es plötzlich wichtig, dass User:innen – zum Beispiel in sozialen Netzwerken – nachvollziehen können, ob ein Artikel wirklich von einer seriösen Quelle stammt?

Hans Brorsen: Das Problem, dass im Internet Falschinformationen verbreitet werden, ist natürlich nicht neu. Doch durch das Aufkommen von generativer Künstlicher Intelligenz ist es jetzt nicht nur einfacher geworden, tolle Inhalte zu erstellen. Programme wie ChatGPT können auch eingesetzt werden, um Fake News und Desinformationen zu produzieren. Schneller, in größerer Menge und sogar personalisiert. Deswegen ist es aus unserer Sicht wichtig, dass User:innen überall dort, wo Nachrichten und Informationen konsumiert werden, herausfinden können, ob diese echt oder falsch sind. Außerdem ist das Buch von einer hawaiianischen Künstlerin illustriert worden.

Reicht es nicht, wenn auf der Webseite zu erkennen ist, welches Medium den Artikel veröffentlicht und wer ihn geschrieben hat?

Jens Brorsen: Die Hälfte des Medienkonsums findet mittlerweile über Drittplattformen statt, vor allem über Social Media – nicht über die Webseite des Mediums, auf der ein Artikel erscheint. Das betrifft vor allem die Generation Z. In Zukunft werden Nachrichten außerdem verstärkt über KI-Chatbots abgefragt werden.

Hans Brorsen: Und selbst eine Webseite, die so aussieht wie die eines seriösen Mediums, kann gefälscht sein. Im vergangenen Jahr sind viele solcher Seiten auf Deutsch aufgetaucht. Sogar die Tagesschau wurde „gedeeptakt“, um Desinformation zu verbreiten.

Ihr arbeitet an einer Web3-Lösung, die derartige Täuschungen verhindern soll. Wie soll diese aussehen?

Jens Brorsen: Wir machen es möglich, die Authentizität von Inhalten anhand von kryptografischen Provenienz-Indikatoren zu überprüfen – und das nicht nur auf den Nachrichten-Webseiten selbst, sondern auch auf Drittplattformen. So können Leser:innen qualitativ hochwertige Nachrichteninhalte anhand der Quelle erkennen und auswählen. Das verhindert Desinformation.

„Kryptografische Provenienz-Indikatoren“? Das müsst ihr genauer erklären.

Jens Brorsen: Die Verfasser:innen bzw. der Verlag signieren mithilfe unserer Software die Nachrichtenartikel mit einem kryptografischen Schlüssel. Diese Nachricht wird dann mathematisch kodiert und samt Signatur auf eine öffentliche Blockchain geschrieben. Mithilfe dieser unveränderbaren Daten können Nutzer:innen die Metadaten des Artikels – also Verfasser:in, Publisher, Veröffentlichungsdatum – und damit die Herkunft des Contents prüfen. Derzeit nutzen wir dafür die Polygon-Blockchain.

Und wie können Nutzer:innen auf diese Informationen zugreifen?

Hans Brorsen: Zunächst ist wichtig: Wir setzen zwar auf die Blockchain als Infrastruktur, aber niemand muss wissen, wie die Blockchain funktioniert, um von unserer Lösung zu profitieren. In der Praxis soll die Nutzung so ablaufen: Neben einer Nachrichtenquelle, zum Beispiel in einem sozialen Netzwerk, findet man einen grünen Haken oder ein anderes Zeichen. Dahinter verbirgt sich ein Link. Klickt man auf dieses Zeichen, öffnet sich ein Fenster, in dem zu lesen ist, wer diesen Nachrichteninhalt signiert hat, welches Medium ihn veröffentlicht hat und wann er das letzte Mal überarbeitet wurde. Durch weitere Klicks kann ich erfahren, was diese Journalistin, dieser Journalist oder auch dieser Verlag sonst noch veröffentlicht hat.

Außerdem wird es möglich, den Text eines Artikels, den man zum Beispiel über WhatsApp weitergeleitet bekommen hat, per Copy-and-Paste bei uns zu überprüfen. Dann stellt man fest, ob es da beispielsweise wirklich eine Signatur gibt. So soll das sogenannte „Sockpuppeting“ verhindert werden, also dass sich jemand für ein seriöses Medium ausgibt, um Propaganda zu betreiben.

Aber wer stellt denn sicher, dass über eure Web3-Lösung nicht auch Fake News „authentifiziert“ werden? Die Technologie kann schließlich nur schwer den Inhalt der Artikel überprüfen.

Hans Brorsen: Wir machen kein Fact-Checking, das ist richtig. Wir vertrauen den Verlagen und Journalist:innen, dass sie ordentlich nach allen Qualitätsmaßstäben gearbeitet haben. Deswegen wollen wir diese Lösung vorerst nur denen geben,

„Wichtig ist: Der Artikel ist nach dem Signieren nicht mehr veränderbar, sonst würden die kryptografisch erzeugten Hashwerte nicht mehr zum ursprünglichen Text passen.“ - Hans Brorsen

die sich dem Pressekodex verpflichtet haben und denen gegenüber der Presserat eine Handhabung in Bezug auf Fake News hat. Es kann natürlich trotzdem passieren, dass etwas Falsches geschrieben wird. Dann greifen die vorhandenen Mechanismen – wie Klarstellung oder Richtigstellung.

Die Leute, die den etablierten Medien nichts mehr glauben, sie als „Lügenpresse“ abstempeln, wird man damit aber nicht überzeugen, oder?

Hans Brorsen: Wir haben in Deutschland das Glück, dass es eine extrem große Presselandschaft gibt, in der sich fast alle in irgendeiner Art und Weise wiederfinden. Und dem Pressekodex haben sich dabei nicht nur die Großen verpflichtet, sondern auch viele Nischenanbieter.

Wir schwingen uns ganz bewusst nicht auf, die Inhalte zu bewerten. Schließlich ist es die eigentliche Aufgabe von Verlagen und Journalist:innen, Informationen zu validieren und einzuordnen. Wir helfen aber dabei, den Wert dieser Arbeit wieder sichtbar zu machen

Wie soll eure Lösung eigentlich für Medienhäuser in der Praxis funktionieren?

Hans Brorsen: Wir stellen ihnen die Werkzeuge zur Verfügung, damit sie ihre Artikel signieren und die entsprechenden Daten auf die Blockchain schreiben können. Danach bekommen die Medienhäuser einen Link zurück, den sie in ihre Nachricht einbauen können. Wichtig dabei ist: Der Artikel ist nach dem Signieren nicht mehr veränderbar, sonst würden die kryptografisch erzeugten Hashwerte nicht mehr zum ursprünglichen Text passen.

Aber was ist, wenn ein Artikel geändert werden muss, ein Update braucht oder – aus welchen Gründen auch immer – offline genommen werden soll?

Hans Brorsen: Das passiert ständig. Wir haben es gelöst, indem der Artikel dann noch einmal signiert wird und die Daten noch einmal auf die Blockchain geschrieben werden. Dadurch ist über unser System auch verfolgbar, ob es die aktuelle Version ist, die man gerade liest. Und man würde darauf hingewiesen werden, wenn man einen alten Artikel sieht.

Eine grundsätzliche Frage: Warum braucht es für eure Lösung überhaupt eine Blockchain? Wäre das alles nicht auch auf klassischen, zentralen Servern umsetzbar? Schließlich müssen die Verlage euch ohnehin vertrauen.

Jens Brorsen: Wir stellen den Verlagen nur die Infrastruktur zur Verfügung, um ihre Daten auf die Blockchain zu schreiben. Und die Blockchain hat den Vorteil, dass alle Daten öffentlich einsehbar sind. Das heißt, Dritte könnten die Authentizität der Artikel auch ohne uns überprüfen oder sogar eigene Tools anbieten, um die Daten abzufragen. Uns braucht man also gar nicht mehr, wenn die Informationen einmal auf der Blockchain sind.

Außerdem bleiben die Informationen auf der Blockchain, selbst wenn es uns nicht mehr geben sollte – und sie können nicht verändert werden. Alles ist also transparent und schafft dadurch Vertrauen.

Wie ist denn bisher die Rückmeldung der Medienhäuser? Besteht Interesse an eurer Lösung?

Hans Brorsen: Die Verlage sehen den Bedarf eigentlich seit dem Vormarsch von generativer KI. Deswegen haben wir sehr gutes Feedback bekommen. Zumal sie durch unsere Lösung auch zusätzliche Nutzer:innen gewinnen könnten, weil diese durch unsere Tools auch andere Inhalte derselben Journalist:innen oder Publisher entdecken können. Und es besteht die Chance, dass authentifizierte Inhalte auf Drittplattformen, zum Beispiel Social Media, besser sichtbar gemacht werden.

Euer Web3-Validierungstool hat nur dann eine echte Chance, wenn die großen Drittplattformen mitmachen – Google, Meta, X. Wieso sollten sie?

Hans Brorsen: Die meisten Leute, die diese Plattformen nutzen, wollen echte Nachrichten lesen und viele sind jetzt schon besorgt, ob sie den Inhalten dort vertrauen können. Allein deswegen sollten die Anbieter schon aus kaufmännischer Sicht motiviert sein, ihren User:innen Möglichkeiten zu geben, die Authentizität von Quellen überprüfen zu können. Das ist sozusagen das Zuckerbrot. Es gibt aber auch die Peitsche: die europäische Gesetzgebung in Form des Digital Services Acts. Dieser besagt, dass Plattformen das Problem der Desinformation in den Griff kriegen müssen, um nicht hohe Bußgelder bezahlen zu müssen.

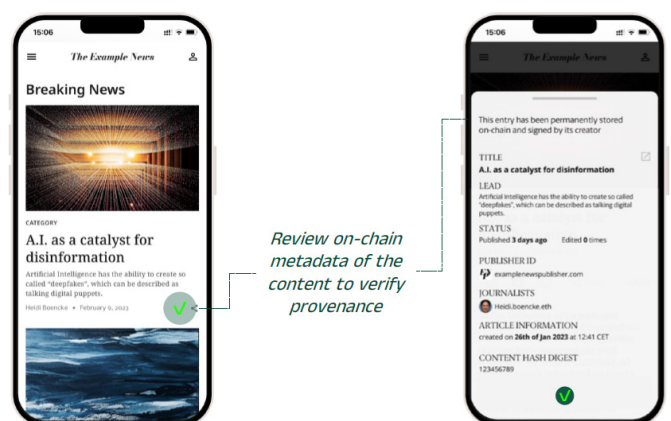


Bild: Screenshot Valid

FALLBEISPIEL 3

IN DER WISSENSCHAFT IM ALLTAGSEINSATZ: DIE BLOXBERG-BLOCKCHAIN AUS MÜNCHEN

Das Projekt Bloxberg, entstanden in der Max-Planck-Gesellschaft in München, beweist, dass Authentifizierungs-Lösungen auf Basis von Web3-Technologien bereits alltagstauglich sind – für die Wissenschaft. Die Anwendungsfälle haben durchaus Ähnlichkeiten mit den Anforderungen der Medienbranche.

Die Herkunft und Authentizität einer Veröffentlichung nachvollziehen zu können, spielt nicht nur im Journalismus eine Rolle. Auch die Wissenschaft beschäftigt sich seit Jahrzehnten mit dem Thema Provenienz. Insbesondere die Belegbarkeit einer Erstveröffentlichung ist für Forscher:innen zentral, um Glaubwürdigkeit und Reputation aufzubauen. Es existieren also durchaus Überschneidungen zwischen den Ansprüchen der wissenschaftlichen und der journalistischen Arbeit.

In der Vergangenheit versuchten Forschungsgesellschaften und nationale Initiativen Provenienz-Lösungen für die Wissenschaft auf Basis interner Datenbanken und Verzeichnisse zu etablieren. Diesen fehlt es jedoch an Offenheit und Transparenz. Daher wird seit 2018 eine Alternative auf Basis von Web3 bzw. der Blockchain-Technologie erprobt. Sie nennt sich Bloxberg, stammt aus München und wurde von der Max-Planck-Gesellschaft mitinitiiert. Zum Trägerkonsortium und den Teilnehmern des großangelegten Experiments gehören internationale Forschungseinrichtungen, darunter die Carnegie Mellon University, die Universität Kassel, die ETH Zürich, die IT University of Copenhagen oder die University of Sarajevo.

Die zentrale Anwendung der Bloxberg-Blockchain ist die Implementierung eines „Proof of Existence“. Sowohl einzelne Forscher:innen als auch Teams aus dem Verbund können also die Existenz von Forschungsergebnissen, Hypothesen und Studien auf der Blockchain verifizieren. Hierfür werden die entsprechenden Forschungsinhalte in einen einmaligen Code – einen Hash – umgewandelt, der auf der Blockchain gespeichert

wird. Der Eintrag kann um Studientitel, Autorennamen, Namen von Forschungseinrichtungen sowie Anmerkungen erweitert werden.

Dies ermöglicht Wissenschaftler:innen, ihre Forschungsbeiträge zu dokumentieren, Nachweise für Rechte an geistigem Eigentum zu schaffen sowie zeitliche Abläufe nachvollziehbar zu machen – ohne diese sofort in kompletten Studien öffentlich publizieren zu müssen. So lässt sich beispielsweise belegen, wer Daten oder Forschungsergebnisse zuerst generiert hat. Aufgrund der dezentralen Architektur der Blockchain ist eine Manipulation der Daten nahezu ausgeschlossen. Die Max-Planck-Gesellschaft und andere Institute haben die Funktionen der Bloxberg-Blockchain bereits in hauseigene Publikationswerkzeuge integriert.

Die Bloxberg-Blockchain könnte laut ihren Entwickler:innen auch zahlreiche weitere Funktionen erlauben. Beispielsweise könnten Diplom- und Doktorarbeiten dort niedergeschrieben werden, genau wie abgeschlossene Peer-Review-Prozesse für Studien. Auch als Rückgrat für ein wissenschaftliches Lizenz- und Tauschsystem könnte die Blockchain fungieren, hoffen die Entwickler:innen an der Max-Planck-Gesellschaft. Rohdaten oder technisches Equipment könnten in Form von digitalen Tokens in die Blockchain eingetragen werden, um über Plattformen angefordert zu werden.

Analoge Funktionen wären – neben der Authentifizierung von Inhalten durch Provenienz-Informationen – auch für den Journalismus vorstellbar. Beispielsweise, indem unabhängige Fact Checker die Publikation eines Mediums verifizieren, was auf der Blockchain vermerkt werden könnte. Auch die Lizenzierung journalistischer Inhalte könnte über eine Blockchain oder ähnliche Datenbanken abgewickelt werden.

FAZIT UND AUSBLICK

TECHNOLOGIE ALLEIN WIRD DIE HERAUSFORDERUNG NICHT LÖSEN

Der Deepdive des Web3-Thinktank zeigt, dass Open-Source-Standards in Verbindung mit Web3-Technologien tatsächlich vielversprechende Möglichkeiten bieten, um die Authentizität und Integrität von digitalem Content zu gewährleisten und damit das Vertrauen in die Informationsquellen zu stärken. Digitale Fingerabdrücke, Echtheitszertifikate oder Wasserzeichen – wie auch immer man die Lösungen konkret benennen möchte – können dabei helfen, Desinformation zu bekämpfen, indem sie die Herkunft und Bearbeitung von Inhalten transparent machen. Auch können sie einen Beitrag dazu leisten, echte und von KI generierte Inhalte unterscheidbar zu machen. Allerdings dürften technologische Lösungen alleine nicht ausreichen, um die Herausforderungen durch Desinformation, möglicherweise weiter angefacht durch KI, zu lösen.

Es braucht darüber hinaus Bildung, Medienkompetenz, professionelles Fact-Checking, Moderation und guten Journalismus, um die Qualität und Glaubwürdigkeit von Informationen zu sichern. Nur so kann eine informierte und kritische Öffentlichkeit entstehen, die sich nicht von manipulierten Inhalten täuschen lässt.

ÜBER UNS

DER WEB3-THINKTANK DES MEDIENNETZWERK BAYERN

Was haben wir als **MedienNetzwerk Bayern** mit Web3 zu tun? Wir haben uns die Frage gestellt: Was können Verlags- und Medienhäuser tun, um erfolgreich ins Web3 mit seinen NFTs, Smart Contracts oder dezentralen autonomen Organisationen auf Basis der Blockchain einzusteigen?

Die Antwort lautet: Wissen aufbauen, Erfahrungen sammeln, experimentieren. Das muss aber nicht jedes Unternehmen für sich allein stemmen, denn im Web3 spielt Kooperation eine zentrale Rolle. Um die Medienbranche zu unterstützen, haben wir gemeinsam mit der Denkfabrik 1E9 den Web3-Thinktank ins Leben gerufen.

Der Web3-Thinktank bietet Medienhäusern in Bayern

- Basis-Input als individueller Inhouse-Workshop und darauf aufbauend:
- Lab-Sessions zur Ideenentwicklung und Konzeption passender Web3-Projekte bis hin zum Prototyping
- Whitepaper
- Offene Veranstaltungen
- Unterstützung bei der Suche nach Expert:innen und Kooperationspartnern für Projekte
- Online-Workshops

Mehr erfahren:



ÜBER DAS MEDIEN NETZWERK BAYERN

Networking ist unser Geschäft! Ein gutes Netzwerk hilft dabei, inspirierende Kontakte zu knüpfen, sich weiterzuentwickeln oder gemeinsam zu schaffen, was alleine nicht geht. Wir, das MedienNetzwerk Bayern, sind eine Initiative für den Medienstandort Bayern. Durch unsere Veranstaltungen und Projekte bringen wir die bayerische Medienbranche zu Trends und Herausforderungen der digitalen Transformation zusammen. Wir vernetzen sowohl die einzelnen Medien-Segmente untereinander, als auch über Branchengrenzen hinweg. Denn durch einen Blick über den Tellerrand lassen sich oft neue Ideen, Kollaborationen oder sogar neue Geschäftsmodelle entwickeln.

Das MedienNetzwerk Bayern ist eine Marke der

**MEDIEN.
BAYERN**

Tochter der



gefördert durch

Bayerische Staatskanzlei



VERZEICHNIS

QUELLEN UND LINKS

Bertelsmann Stiftung: Desinformation: Herausforderung für die Demokratie, 10. August 2023, aufgerufen am 11. Oktober 2023, <https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/desinformation-herausforderung-fuer-die-demokratie>

Canon: Reuters new proof of concept employs authentication system to securely capture, store and verify photographs, 31. August 2023, aufgerufen am 11. Oktober 2023, <https://global.canon/en/news/2023/20220831.html>

Coalition for Content Provenance and Authenticity, aufgerufen am 11. Oktober 2023, <https://c2pa.org/>

Coalition for Content Provenance and Authenticity: C2PA Specifications, aufgerufen am 11. Oktober 2023, <https://c2pa.org/specifications/specifications/1.3/index.html>

Cointelegraph: Blockchain key to verifying authenticity of real-world media – Nodle, 5. Oktober 2023, aufgerufen am 11. Oktober 2023, <https://cointelegraph.com/news/blockchain-to-verify-real-world-media-authenticity-nodle>

Content Authenticity Initiative, aufgerufen am 11. Oktober 2023, <https://contentauthenticity.org/>

Content Credentials / Content Authenticity Initiative: Verify, 2023, aufgerufen am 11. Oktober 2023, <https://contentcredentials.org/verify>

Die Bundesregierung: Was ist Desinformation?, 4. September 2023, aufgerufen am 11. Oktober 2023, <https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/was-ist-desinformation-1875148>

Die Bundesregierung: Kann ChatGPT Desinformation erkennen?, 12. Juli 2023, aufgerufen am 11. Oktober 2023, <https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/chatgpt-desinformation-2197678>

European Commission: The 2022 Code of Practice on Disinformation, 2022, aufgerufen am 11. Oktober 2023, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>

Europol Innovation Lab: Facing reality? Law enforcement and the challenge of deepfakes, 2022, aufgerufen am 11. Oktober 2023, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf

Filecoin, aufgerufen am 11. Oktober 2023, <https://filecoin.io/>

IPFS, aufgerufen am 11. Oktober 2023, <https://ipfs.tech/>

Josh A. Goldstein et al.: Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations, Januar 2023, aufgerufen am 11. Oktober 2023, <https://arxiv.org/abs/2301.04246>

Leica: Partnership for greater trust in digital photography: Leica and Content Authenticity Initiative, aufgerufen am 11. Oktober 2023, <https://leica-camera.com/en-int/news/partnership-greater-trust-digital-photography-leica-and-content-authenticity-initiative>

Licium, aufgerufen am 11. Oktober 2023, <https://licium.com/>

Nikon: Nikon to exhibit a sample camera specially equipped with an image provenance function at Adobe MAX 2022, 19. Oktober 2022, aufgerufen am 11. Oktober 2023, https://www.nikon.com/company/news/2022/1019_exhibition_01.html

Nina Schick, aufgerufen am 11. Oktober 2023, <https://ninaschick.org/>

Numbers Protocol, aufgerufen am 11. Oktober 2023, <https://www.numbersprotocol.io/>

OpenTimestamps, aufgerufen am 11. Oktober 2023, <https://opentimestamps.org/>

Project Origin, aufgerufen am 11. Oktober 2023, <https://www.originproject.info/>

ProvenDB, aufgerufen am 11. Oktober 2023, <https://www.provencdb.com/>

Reddit (r/midjourney): The Pope Drip, März 2023, aufgerufen am 11. Oktober 2023, https://www.reddit.com/r/midjourney/comments/120vhdc/the_pope_drip/

Reuters: Preserving trust in photojournalism through authentication technology, 2023, aufgerufen am 11. Oktober 2023, <https://www.reutersagency.com/authenticity-poc>

Rolling Stone: The DJ and the War Crimes, 2022, aufgerufen am 11. Oktober 2023, <https://investigation.rollingstone.com/dj-photo-war-crimes-bosnia/>

Starling Lab, aufgerufen am 11. Oktober 2023, <https://www.starlinglab.org/>

Starling Lab: 78 Days – Creating a Photographic Archive of Trust, 2021, aufgerufen am 11. Oktober 2023, <https://www.starlinglab.org/78days/>

Storj, aufgerufen am 11. Oktober 2023, <https://www.storj.io/>

Tagesschau.de: Flut an getarnten Desinformationen, 7. November 2022, aufgerufen am 11. Oktober 2023, <https://www.tagesschau.de/faktenfinder/fake-news-serioese-marken-103.html>

Truepic: Truepic Lens, aufgerufen am 11. Oktober 2023, <https://truepic.com/truepic-lens/>

Valid, aufgerufen am 11. Oktober 2023, <https://valid.tech/>

XPLR: Media in Bavaria, 1E9: Web3 Studie – Was kommt auf die Medienbranche zu?, Oktober 2022, aufgerufen am 11. Oktober 2023, <https://www.xplr-media.com/de/web3-studie.html>



WEB3-THINKTANK

Medien.Bayern GmbH | MedienNetzwerk Bayern
August-Everding-Straße 25 / 81671 München
Tel.: 089 68999-0 / E-Mail: info@mediennetzwerk.bayern
www.mediennetzwerk-bayern.de/web3